EXHIBIT A

Data ONTAP® 7.2
Network Management Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: http://www.netapp.com

Part number 210-03535_A0
Updated for Data ONTAP 7.2.2 on 22 March 2007

Copyright and trademark information

Copyright information

Trademark information

Table of Contents

Host-Name Resolution 4

About this chapter

This chapter discusses how you can use the Data ONTAP configuration files, Domain Name System (DNS), and Network Information Service (NIS) to resolve host names.

Topics in this chapter

This chapter discusses the following topics:

Maintenance of host information

Ways to maintain host information

Host information can be maintained in one or all of the following ways in Data ONTAP:

- In the /etc/hosts file on your storage system's default volume

  For detailed information, see "Using the /etc/hosts file to maintain host information" on page 87.
- On a Domain Name System (DNS) server

  For detailed information, "Using DNS to maintain host information" on page 91.
- On a Network Information Service (NIS) server

  For detailed information, see "Using NIS to maintain host information" on page 101.

Search order for host information

If you use more than one of the above ways to maintain host information, the ways are used in the order determined by the /etc/nsswitch.conf file. For detailed information about this file, see "Changing the host name search order" on page 110.

The role of host-name resolution in Data ONTAP

Data ONTAP relies on correct host-name resolution to provide basic connectivity for storage systems on the network, including

- Processing NFS mount requests
- Establishing CIFS sessions
- Authenticating Remote Shell (RSH) protocol sessions to storage systems

If you are unable to access storage system data or establish sessions, there might be problems with host-name resolution on your storage system or on a name server.

Using the /etc/hosts file to maintain host information

About the /etc/hosts file

Data ONTAP uses the /etc/hosts file to resolve host names to IP addresses, including host names used in any of the following files:

- /etc/rc
- /etc/syslog.conf
- /etc/exports
- /etc/netgroup
- /etc/hosts.equiv

You must ensure that the /etc/hosts file is kept up-to-date. If you update the file, you do not need to reboot your storage system—the changes to the file take effect immediately.

When Data ONTAP is first installed, the /etc/hosts file is automatically created with default entries for the following interfaces:

- localhost
- All interfaces on your storage system

Note

The /etc/hosts file resolves the host names for the storage system it is configured on. This file cannot be used by other systems for name resolution.

For more information on file format, see the na_hosts(5) man page.

Ways to add entries to the /etc/hosts file

You can add IP address and hostname entries in the /etc/hosts file in the following two ways:

- Locally

  You might want to add entries to the local /etc/hosts file if the number of entries is small. You can do so in the following ways:

  - At the command line

    See "Editing the /etc/hosts file manually" on page 88.
  - Using FilerView

    See "Editing the /etc/hosts file with FilerView" on page 89.

- Remotely using the NIS makefile master

  If the number of entries is large and you have access to an NIS makefile master, you might want to use the makefile master to create the /etc/hosts file. This method prevents errors that could be introduced in the manual creation process. For details, see "Creating /etc/hosts from the NIS master" on page 89.

  Note

  Using NIS to distribute the /etc/hosts file is different from looking up host names on an NIS server. For more information about network lookups, see "Using NIS to maintain host information" on page 101.

/etc/hosts file hard limits

The following are hard limits for the `/etc/hosts` file:

- Maximum line size is 1022 characters.
- Maximum number of aliases is 34.
- There is no file size limit.

Note

The line size limit includes the end of line character. You can enter up to 1021 characters per line.

Editing the /etc/hosts file manually

To edit the /etc/hosts file manually, complete the following steps.

Step	Action
1	From a workstation that has access to your storage system's root volume, open the /etc/hosts file using a text editor.
2	Edit the file to your needs. The format of the file is as follows: *IP address Host-name aliases*
3	Save the file.

Example: The following shows how the entries might look in the /etc/hosts file on a storage system:

```
192.16.3.145    toaster    toaster-e0
192.16.4.155    toaster-e2
192.16.5.165    toaster-e4
192.16.6.175    toaster-e8
```

In the first line, your storage system's host name itself is used as an alias for the first network interface. That is, network traffic addressed to toaster will be received on the toaster-e0 interface.

Editing the /etc/hosts file with FilerView

To edit the /etc/hosts file with FilerView, complete the following steps.

Step	Action
1	In FilerView, click Network in the list on the left.
2	In the list under Network, click Manage Hosts File.
3	Click in the hosts window, then click Insert.
4	Complete the fields in the Create a New /etc/hosts Line window for each host you wish to add and click OK.
5	Click Apply in the Manage Hosts File window.

Creating /etc/hosts from the NIS master

To modify the makefile for the NIS master to create a hosts file and copy it to the /etc directory on your storage system's default volume, complete the following steps.

Step	Action
1	On the NIS server, open the NIS makefile with an editor.
2	Locate the section for hosts.time.

Step	Action

3	Add the following lines at the end of the hosts.time section, replacing *dirname* with a directory name of your choice, and *toaster 1*, *toaster2*, and so on with names of your storage systems:
	
	`@mntdir=/tmp/dirname_etc_mnt_$$$$;\`
	`if [ ! -d $$mntdir ]; then rm -f $$mntdir; \`
	`mkdir $$mntdir; fi;\`
	`for s_system in toaster1 toaster2 toaster3 ; do \`
	`mount $$s_system:/etc $$mntdir;\`
	`mv $$mntdir/hosts $$mntdir/hosts.bak;\`
	`cp /etc/hosts $$mntdir/hosts;\`
	`umount $$mntdir;\`
	`done;\`
	`rmdir $$mntdir`

4	Save the NIS makefile. The /etc/hosts file on your storage system is updated whenever the NIS makefile is run.

/etc/netgroup file hard limits

When editing the /etc/netgroup file, please observe these hard limits:

- Maximum entry size is 4096.
- Maximum netgroup nesting limit is 1000.
- There is no file size limit.

Note

The entry size limit includes the end of line character. You can add up to 4095 characters per entry.

Using DNS to maintain host information

Advantage of using DNS

DNS enables you to maintain host information centrally. As a result, you do not have to update the /etc/hosts file every time you add a new host to the network. If you have several storage systems on your network, maintaining host information centrally saves you from updating the /etc/hosts file on each storage system every time you add or delete a host.

A conventional storage system policy for efficient host-name resolution is to do both of the following:

- Maintain a short /etc/hosts file containing local interfaces, as described in "Ways to add entries to the /etc/hosts file" on page 87.
- Enable DNS with DNS caching, as described in "About configuring DNS" on page 91 and "What DNS name caching does" on page 95.

About configuring DNS

You can configure your storage system to use one or more DNS servers either during the `setup` procedure or later using the command line or FilerView.

If you configure DNS during the `setup` procedure, your storage system's DNS domain name and name server addresses are configured

- Automatically if you use Dynamic Host Configuration Protocol (DHCP) to configure onboard interfaces
- Manually if you do not use DHCP—you must enter the values when prompted

If you configure DNS later, you need to take these actions:

- Specify DNS name servers.
- Specify the DNS domain name of your storage system.
- Enable DNS on your storage system.

You can enable DNS and set DNS configuration values in either of these ways:

- Using FilerView

  See "Configuring DNS with FilerView" on page 92.

- At the command line

  See the appropriate instructions:

  - "Creating or editing /etc/resolv.conf" on page 94
  - "Specifying the DNS domain name" on page 94
  - "Disabling or enabling DNS" on page 95

If you want to use primarily DNS for host-name resolution, specify it ahead of other methods in the hosts map in the /etc/nsswitch.conf file. For information about how to edit the nsswitch.conf file, see "Changing the host name search order" on page 110.

Correct host-name resolution depends on the correct configuration of the DNS server. If you experience problems with host-name resolution or data availability, check the DNS server in addition to local networking.

For more information about storage system DNS resolution of host names, see the na_dns(8) man page.

Configuring DNS with FilerView

To set or modify DNS configuration values with FilerView, complete the following steps.

Step	Action
1	In FilerView, click Network in the list on the left.
2	In the list under Network, click Manage DNS and NIS Name Service.

Step	Action	
3	**If you want to....**	**Then...**
	Enable DNS	Select Yes in the DNS Enabled field.
	Set or modify the DNS domain name	Enter a name in the DNS Domain Name field. Examples of configuration values are listed in "Specifying the DNS domain name" on page 94.
	Specify or modify DNS servers	Enter up to three IP addresses in the DNS Servers fields. Examples of configuration values are listed in "Creating or editing /etc/resolv.conf" on page 94.
	Specify or modify the search list for host name lookup	Enter a name in the DNS Domain Search field.

Creating or editing /etc/resolv.conf

To create or edit the /etc/resolv.conf file, complete the following step.

Step	Action	
1	**If...**	**Then...**

	You are creating the /etc/resolv.conf file	Using a text editor, create the /etc/resolv.conf file in the root volume. The file can consist of up to three lines, each specifying a name server host in the following format:
		`nameserver ip_address`
		Example:
		`nameserver 192.9.200.10`
		`nameserver 192.9.200.20`
		`nameserver 192.9.200.30`

	You are editing the /etc/resolv.conf file	From a workstation that has access to your storage system's root volume, edit the /etc/resolv.conf file using a text editor.

You can optionally set or modify the domain search list for DNS host name lookup. For more information, see the na_resolv.conf(5) man page

/etc/resolv.conf hard limits

The following are the NFS hard limits for the /etc/resolv.conf command.

- Maximum line size is 256.
- Maximum number of name servers is 3.
- Maximum domain name length is 256.
- Maximum search domains limit is 6. The total number of characters for all seach domains cannot exceed 256.
- No file size limit.

Note

The line size limit includes the end of line character. You can add up to 255 characters per line.

Specifying the DNS domain name

To specify or change the DNS domain name, complete the following step at your storage system command line.

Step	Action
1	Enter the following command: **`options dns.domainname domain`** *domain* is the new domain name, which follows your storage system's host name in the fully qualified domain name. For example, the domain name of the storage system system1.company.com is company.com.

Disabling or enabling DNS

To disable or enable DNS, complete the following step at your storage system command line.

Step	Action
1	Enter the following command: **`options dns.enable {off|on}`** Use `off` to disable DNS or `on` to enable DNS.

If you did not configure DNS during the Data ONTAP `setup` procedure, DNS is disabled by default.

Once enabled, DNS should be disabled only when you change host-name resolution procedures or when you troubleshoot problems with the DNS name server or Windows Active Directory server.

Note

Your storage system's CIFS implementation depends on DNS to provide the Windows Active Directory service. Therefore, disabling DNS might interrupt CIFS services.

What DNS name caching does

DNS name caching enables the DNS name resolver to speed up the process by which it converts host names into IP addresses. DNS name caching stores DNS requests by caching them so that they are easy to find the next time. Name caching improves DNS performance in the case of name server failure as well as reducing the time it takes for cluster takeover and giveback.

DNS name caching is enabled by default.

Disabling or enabling DNS name caching

To disable or enable DNS name caching, complete the following step at your storage system command line.

Attention

Disabling DNS name caching clears the DNS name cache.

Step	Action
1	Enter the following command: `options dns.cache.enable {on|off}` Use `on` to enable DNS name caching or `off` to disable DNS name caching.

Flushing the DNS cache

Entries in the DNS cache have a set expiration. If an entry that has expired is needed again, your storage system contacts the DNS server to get an updated entry. However, if a DNS entry changes before it has expired, you must flush the DNS cache to force the storage system to get the new DNS record.

If some of your DNS records change often, you should make sure that your DNS server transmits them with a low Time To Live (TTL). (You set the TTL in the DNS server.) You can also disable DNS caching on your storage system with the `dns.cache.enable` option, but doing so might reduce performance.

To flush the DNS cache, complete the following step.

Step	Action
1	Enter the following command: `dns flush`

Displaying DNS information

You can display the following types of DNS information:

- Status of the DNS resolver
- List of DNS servers configured in the /etc/resolv.conf file
- State of each DNS server

- Timestamp when the DNS server was last polled
- Average round-trip time of a DNS query
- Total number of DNS queries made
- Number of failed DNS queries
- Default domain configured on your storage system
- List of other domains that will be used with unqualified names for name lookup

To display DNS information, complete the following step.

Step	Action
1	Enter the following command: **`dns info`**

For more information about the `dns info` display, see the na_dns(1) man page.

Using dynamic DNS to update host information

About dynamic DNS updates

Dynamic DNS updates enable your storage system to send new or changed DNS information to the primary master DNS server for your storage system's zone.

Need for dynamic DNS updates

Without dynamic DNS updates, system administrators have to manually add DNS information (DNS name and IP address) to the identified DNS servers when a new system is brought online or when existing DNS information changes. This process is not only slow, but also error-prone.

Additionally, in a disaster-recovery situation when a storage system with a large number of vFiler units is brought online, manual configuration of DNS information for those vFiler units can result in a longer-than-needed downtime.

By enabling dynamic DNS updates on your storage system, you allow your storage system to automatically send information to the DNS servers as soon as the information changes on the system.

For example, if you want to change the IP address on interface e0 of StorageSystem1, you can simply configure e0 with the new IP address. StorageSystem1 automatically sends updated information to primary master DNS server for StorageSystem1.

How dynamic DNS updates work in Data ONTAP

If dynamic DNS updates are enabled on your storage system, it periodically sends updates to the primary master DNS server for its zone. Your storage system finds out the primary master DNS server for its zone by querying the DNS servers configured in storage system's /etc/resolv.conf file. The primary master DNS server might be different from the ones configured in your storage system's /etc/resolv.conf file.

By default, periodic updates are sent every 12 hours. A time-to-live (TTL) value is assigned to every DNS update sent from your storage system. The TTL value defines the time for which a DNS entry is valid on the DNS server. By default, the TTL value is set to 24 hours, and you can change it.

In addition to periodic updates, DNS updates are also sent if any DNS information changes on your storage system.

When your storage system sends an update to the DNS server, it waits up to five minutes to receive an acknowledgement of the update from the server. If it does not receive an acknowledgement, the storage system sends the update again. This time, the storage system doubles the waiting interval (to 10 minutes), before sending the update. The storage system continues to double the waiting interval with each retry until a waiting interval of 160 minutes or TTL/2, whichever is less, is reached.

Support for dynamic DNS updates in Data ONTAP

When using dynamic DNS updates in Data ONTAP, the following conditions apply:

- By default, dynamic DNS updates are disabled in Data ONTAP.
- Dynamic DNS updates are supported on UNIX and Windows systems.
- On Windows DNS servers, secure dynamic DNS updates can be used to prevent malicious updates on the DNS servers. Kerberos is used to authenticate updates.

  Even if secure dynamic DNS updates are enabled, your storage system initially tries sending updates in clear text. If the DNS server is configured to accept only secure updates, the updates sent in clear text are rejected. Upon rejection, the storage system sends secure DNS updates.
- For secure dynamic DNS updates, your storage system must have CIFS running and must be using Windows Domain authentication.
- Dynamic DNS updates *can* be sent for the following:
  - Vif and VLAN interfaces
  - vFiler units
- You cannot set TTL values for individual vFiler units. All vFiler units inherit the TTL value set for vFiler0, which is the default vFiler unit and is the same as the physical storage system.
- DHCP addresses *cannot* be dynamically updated.
- In a takeover situation, the hosting storage system is responsible for sending DNS updates for IP addresses for which it is responding.

Enabling dynamic DNS updates

To enable your storage system to send dynamic DNS updates automatically, complete the following step on your storage system.

Step	Action
1	Enter the following command: **`options dns.update.enable [ off | on | secure ]`** `Off`—Disable dynamic DNS updates `On`—Enable dynamic DNS updates `Secure`—Enable secure dynamic DNS updates **Note** Secure dynamic DNS updates are supported for Windows DNS servers only.

Changing the time-to-live setting for DNS entries

To change the TTL for the DNS entries, complete the following step.

Step	Action
1	Enter the following command: **`options dns.update.ttl time`** where *time* can be set in seconds (`s`), minutes (`m`), or hours (`h`) with a minimum value of 600 seconds and a maximum value of 24 hours. For example, to set the TTL to two hours, enter the following command: `options dns.update.ttl 2h`

Using NIS to maintain host information

Advantage of using NIS

Like DNS, NIS enables you to centrally maintain host information. NIS provides two methods for storage system host-name resolution:

- Using a makefile master on the NIS server, which creates a /etc/hosts file and copies it to your storage system's default volume for local host name lookup

  This method is described in "Creating /etc/hosts from the NIS master" on page 89.
- Using a hosts map, maintained as a database on the NIS server, which your storage system queries in a host lookup request across the network

  This method is described in this section.

NIS also enables you to maintain user information. For more information, see the Data ONTAP *System Administration Guide*.

Using NIS slave for name resolution

Host-name resolution using a hosts map can have a performance impact, because each query for the hosts map is sent across the network to the NIS server. To improve performance, you can enable an NIS slave on your storage system.

The NIS slave establishes a contact with an NIS master server and does the following two tasks:

- Downloads the maps from the NIS master server

  Once the maps have been downloaded, they are stored in the /etc/yp/*nis_domain_name*/ directory. All NIS requests from your storage system are then serviced by the NIS slave using these maps. The NIS slave checks the NIS master every 45 minutes for any changes to the maps. If there are changes, they are downloaded.
- Listens for updates from the NIS master

  When the maps on the NIS master are changed, the NIS master administrator can choose to notify all slaves. Therefore, in addition to periodically checking for updates from the NIS master, the NIS slave also listens for updates from master.

Note

The NIS slave does not respond to remote NIS client requests and thus cannot be used by other NIS clients for name lookups.

Selection of an NIS master

When the NIS slave is enabled on your storage system, the NIS servers listed with the `nis.servers` option are contacted to determine the master NIS server. The NIS master can be different from the servers listed with the `nis.servers` option. If that is the case, the servers listed with the `nis.servers` option inform the slave about the master server.

Note

Either the NIS server must have an entry in the hosts map for the master or the /etc/hosts file on your storage system must be able to resolve the IP address of the master. Otherwise, the NIS slave on the storage system cannot contact the master.

Guidelines for using the NIS slave

Keep the following guidelines in mind when using the NIS slave on your storage system:

- The root volume of your storage system must have sufficient space to download maps for the NIS slave. Typically, the space required in the root volume is same as the size of the maps on the NIS server.

  If the root volume does not have enough space to download maps, the following occurs:

  - An error message is displayed informing you that the space on the disk is not sufficient to download or update the maps from the NIS master.
  - If the maps cannot be *downloaded*, the NIS slave is disabled. Your storage system switches to using hosts map on the NIS server for name resolution.
  - If the maps cannot be *updated*, your storage system continues to use the old maps.

- If the NIS master server was started with the `-d` option or if the `hosts.byname` and `hosts.byaddr` maps are generated with the `-b` option, your storage system must have DNS enabled, DNS servers must be configured, and the hosts entry in the /etc/nswitch.conf file must contain DNS as an option to use for host name lookup.

  If you have your NIS server configured to do host name lookups using DNS or if you use DNS to resolve names that cannot be first resolved using the `hosts.by*` maps, using the NIS slave causes those lookups to fail, because when the NIS slave is used, all lookups are performed locally using the downloaded maps. However, if you configure DNS on your storage system as described previously, the lookups succeed.

- You can use the NIS slave for the following:
  - Vif and VLAN interfaces
  - vFiler units
  - Storage system clusters

Note

Ensure that the `nis.servers` options value is the same on both cluster nodes and that the /etc/hosts file on both cluster nodes can resolve the name of the NIS master server.

About configuring NIS for host lookups

You can configure your storage system to use one or more NIS servers either during the `setup` procedure or later using the Data ONTAP command line or FilerView.

If you configure NIS later, you need to do all of the following:

- Specify the NIS server to which your storage system should bind
- Specify the NIS domain name of your storage system
- Enable NIS on your storage system

You cannot configure the NIS slave during the `setup` procedure. To configure the NIS slave after the `setup` procedure is complete, you need to enable NIS slave by setting the option `nis.slave.enable` to On. For more information about enabling NIS slave, see "Enabling an NIS slave on your storage system" on page 107.

Data ONTAP interfaces to configure NIS

You can enable NIS and set NIS configuration values in either of these ways:

- Using FilerView

  See "Configuring NIS with FilerView" on page 104.

  You cannot use FilerView to configure the NIS slave.
- At the command line

  See the appropriate instructions:
  - "Specifying NIS servers to bind to" on page 105
  - "Specifying the NIS domain name" on page 105
  - "Enabling or disabling NIS using the command-line interface" on page 105

If you want to use primarily NIS for host-name resolution, specify it ahead of other methods in the hosts map in the /etc/nsswitch.conf file. For information about editing the /etc/nsswitch.conf file, see "Changing the host name search order" on page 110.

Correct host-name resolution depends on the correct configuration of the NIS server. If you experience problems with host-name resolution or data availability, check the NIS server in addition to local networking.

For more information about your storage system's NIS client, see the na_nis(8) man page.

Configuring NIS with FilerView

To set or modify NIS configuration values with FilerView, complete the following steps.

Step	Action	
1	In FilerView, click Network in the list on the left.	
2	In the list under Network, click Manage DNS and NIS Name Service.	
3	**If you want to....**	**Then...**
	Enable or disable NIS	Select Yes or No in the NIS Enabled field.
	Set or modify the NIS domain name	Enter a name in the NIS Domain Name field. Examples of configuration values are listed in "Specifying the NIS domain name" on page 105.
	Specify or modify NIS servers	Enter one or more IP addresses in the NIS Servers fields. Examples of configuration values are listed in "Specifying NIS servers to bind to" on page 105.

Enabling or disabling NIS using the command-line interface

To enable or disable NIS on your storage system, complete the following step.

Step	Action
1	Enter the following command: `options nis.enable {on|off}` Use `On` to enable and `Off` to disable NIS.

Specifying the NIS domain name

To specify the NIS domain name, complete the following step.

Step	Action
1	Enter the following command: `options nis.domainname domain` *domain* is the NIS domain name to which your storage system belongs; for example, typical NIS domain names might be *sales* or *marketing*. The NIS domain name is usually not the same as the DNS domain name.

Specifying NIS servers to bind to

You can specify an ordered list of NIS servers to which you want your storage system to bind. The list should begin with the closest NIS server (closest in network terms) and end with the furthest one.

To specify an ordered list of NIS servers you want your storage system to bind to, complete the following step.

Note

You can specify NIS servers by IP address or host name. If host names are used, make sure each host name, along with its IP address, is listed in the /etc/hosts file of your storage system. Otherwise, the binding with host name will fail.

Step	Action
1	Enter the following command to specify the NIS servers and their order: **options nis.servers *ip_address, server_name,* *** The asterisk (*) specifies that broadcast is used to bind to NIS servers if the servers in the list are not responding. This is the default. If you do not specify broadcasting (that is, if you do not add the asterisk), and none of the listed servers is responding, NIS services are disrupted until one of the preferred servers responds. You can specify only IPv4 addresses or server names that resolve to IPv4 addresses using the /etc/hosts file on your storage system. **Attention** Using the NIS broadcast feature can incur security risks.

Example of specifying NIS servers to bind to: The following lists two servers and uses the broadcast default:

```
options nis.servers 172.15.16.1,nisserver-1,*
```

Your storage system first tries to bind to 172.15.16.1. If the binding fails, the storage system tries to bind to nisserver-1. If this binding also fails, the storage system binds to any server that responds to the broadcast. While bound to the NIS server that responded to the broadcast, the storage system continues to poll the preferred servers. As soon as one of the preferred servers is found, the storage system binds to the preferred server.

Enabling an NIS slave on your storage system

To enable an NIS slave on your storage system, complete the following step.

Step	Action
1	Enter the following command: `options nis.slave.enable {on|off}` Use `on` to enable the NIS slave and `off` to disable it. **Note** If the NIS slave is disabled, your storage system reverts back to the original configuration, in which it contacts an NIS server to resolve host names.

Displaying NIS information

To display NIS information, complete the following step.

Step	Action
1	Enter the following command: `nis info`

For more information about the `nis info` command and resulting display, see the na_nis(1) man page.

You can display the following types of NIS information:

- NIS domain name
- Last time the local group cache was updated
- The following information about each NIS server that was polled by your storage system:
  - IP address of the NIS server
  - Type of NIS server
  - State of the NIS server
  - Whether your storage system is bound to the NIS server
  - Time of polling
- Information about the NIS netgroup cache
  - a. The status of the cache
  - b. The status of the "*.*" entry in the cache

- c. The status of the "*.nisdomain" entry in the cache
- Whether an NIS slave is enabled
- NIS master server
- Last time the NIS map was checked by the NIS slave
- NIS performance statistics:
  - Number of YP lookup network retransmissions
  - Total time spent in YP lookups
  - Number of network retransmissions
  - Minimum time spent in a YP lookup
  - Maximum time spent in a YP lookup
  - Average time spent in a YP lookup
- Response statistics for the three most recent YP lookups

Example:

The following example shows the statistics provided by the `nis info` command:

```
system1*> nis info
NIS domain is lab.netapp.com

  NIS group cache has been disabled

   IP Address      Type  State  Bound        Last Polled
Client calls   Became Active
------------------------------------------------------------------------
----------------------------
172.16.100.72   PREF  ALIVE  YES   Mon Jan 23 23:11:14 GMT 2006
0   Fri Jan 20 22:25:47 GMT 2006


                NIS Performance Statistics:
        Number of YP Lookups: 153
        Total time spent in YP Lookups: 684 ms, 656 us
        Number of network re-transmissions: 0
        Minimum time spent in a YP Lookup: 0 ms, 1 us
        Maximum time spent in a YP Lookup: 469 ms, 991 us
        Average time spent in YP Lookups: 4 ms, 474 us

                3 Most Recent Lookups:
        [0] Lookup time: 0 ms, 1 us     Number of network re-
transmissions: 0
        [1] Lookup time: 5 ms, 993 us   Number of network re-
transmissions: 0
```

```
        [2] Lookup time: 0 ms, 1 us     Number of network re-
transmissions: 0

NIS netgroup (*.* and *.nisdomain) cache status: Netgroup cache:
uninitialized
*.* eCode: 0
*.nisdomain eCode: 0

 NIS Slave disabled
```

NIS administrative commands

Data ONTAP supports the standard NIS administrative commands listed in the following table. For more information, see each command's man page.

Command	Function
ypcat	Prints an entire NIS map
ypgroup	Displays the NIS group cache entries
ypmatch	Looks up specific entries in an NIS map
ypwhich	Returns the name of the current NIS server

Changing the host name search order

How the host name search order is determined

If you use more than one method for host-name resolution, you must specify the order in which each name resolution service is used. This order is specified in the /etc/nsswitch.conf file in your storage system's root volume.

The default /etc/nsswitch.conf file

Data ONTAP creates a default nsswitch.conf file when you run the `setup` command on your storage system. The contents of the default file are as follows:

```
hosts: files nis dns
passwd: files nis ldap
netgroup: files nis ldap
group: files nis ldap
shadow: files nis
```

Note

Only the hosts entry in the /etc/nsswitch.conf file pertains to host-name resolution. For information about other entries, see the Data ONTAP *System Administration Guide* and the na_nsswitch.conf(5) man page.

By default, the host information is searched in the following order:

- /etc/hosts file
- NIS
- DNS

If you want to change this order, you can do so in either of these ways:

- By using FilerView

  See "Changing the host name search order with FilerView" on page 111.
- By editing the /etc/nsswitch.conf file

  See "Editing the /etc/nsswitch.conf file" on page 111.

Changing the host name search order with FilerView

To change the host name search order with FilerView, complete the following steps.

Step	Action
1	In FilerView, click Network in the list on the left.
2	In the list under Network, click Manage DNS and NIS Name Service.
3	In the Name Service section, select the desired values in the Hosts drop-down lists.

Editing the /etc/nsswitch.conf file

To change the order in which Data ONTAP searches for host information, complete the following steps.

Step	Action
1	If the /etc/nsswitch.conf file does not exist in your storage system's root volume, create it.
2	Edit the file, entering each line in the following format: `map: service ...` *map* for the host-name resolution service is `hosts`. *service* is one or more of the following: `files, dns, nis`. For example, to change the resolution order to use NIS exclusively, change the hosts line to read as follows: hosts: nis
3	Save the file.

Storage System Monitoring Using SNMP 5

About this chapter

This chapter describes how Data ONTAP supports SNMP on your storage system and how you can use SNMP to monitor your storage system.

Topics in this chapter

This chapter discusses the following topics:

Understanding SNMP implementation in Data ONTAP

SNMP process

If Simple Network Management Protocol (SNMP) is enabled in Data ONTAP, SNMP managers can query your storage system's SNMP agent for information (specified in your storage system's MIBs or the MIB-II specification). In response, the SNMP agent gathers information and forwards it to the SNMP managers using the SNMP protocol. The SNMP agent also generates trap notifications whenever specific events occur and sends these traps to the SNMP managers. The SNMP managers can then carry out actions based on information received in the trap notifications.

SNMP agent and MIB groups supported

For diagnostic and other network management services, Data ONTAP provides an SNMP agent compatible with SNMP version 1. This agent supports the MIB-II specification and the MIBs of your storage system. The following MIB-II groups are supported:

- System
- Interfaces
- Address translation
- IP
- ICMP
- TCP
- UDP
- SNMP

Note

Transmission and EGP MIB-II groups are not supported.

For more information about protocol support, see the na_snmpd(8) man page.

Types of traps in Data ONTAP

There are two types of traps in Data ONTAP:

- Built-in—Built-in traps are predefined in Data ONTAP and are automatically sent to the network management stations on the traphost list if an event occurs. These traps are based on one of the following:
  - RFC 1213, which defines traps such as coldStart, linkDown, linkUp, and authenticationFailure

- Specific traps defined in the custom MIB, such as diskFailedShutdown, cpuTooBusy, and volumeNearlyFull

For more information, see "Understanding traps in Data ONTAP" on page 116.

- User-defined—User-defined traps exist only after they are defined by a series of `snmp traps` commands or the FilerView SNMP Traps windows. These traps are sent using proxy trap ID numbers 11 through 18, which correspond to a trap's MIB priority.

  For more information, see "Creating SNMP traps" on page 129.

About the Data ONTAP MIBs

A Management Information Base (MIB) file is a textual description of SNMP objects and traps. Therefore, the Data ONTAP MIB files document the SNMP capabilities of the Data ONTAP version running on your storage system. MIBs are not configuration files—that is, values in the MIBs are not read by Data ONTAP, and changes to the MIB files do not affect SNMP functionality.

Data ONTAP provides two MIB files:

- A custom MIB (/etc/mib/netapp.mib)

  See "Contents of the custom MIB" on page 119.

- An internet SCSI (iSCSI) MIB (/etc/mib/iscsi.mib)

  See"Contents of the iSCSI MIB" on page 122.

Data ONTAP also provides a short cross-reference between object identifiers (OIDs) and object short names in the /etc/mib/traps.dat file. This is useful for creating user-defined traps, as discussed in "Defining or modifying a trap" on page 131.

Note

The latest versions of the Data ONTAP MIBs and traps.dat files are available online on the NetApp on the Web™ (NOW) site at http://now.netapp.com/NOW/download/tools/mib/filer.shtml. However, the versions of these files on the web site do not necessarily correspond to the SNMP capabilities of your Data ONTAP version. They are provided to help you evaluate SNMP features in the latest Data ONTAP release.

Understanding traps in Data ONTAP

About traps

Traps are mechanisms that alert you to significant events on your storage system. If SNMP is configured, traps are fired when a defined event, such as a network traffic interruption or line power failure, occurs. Trap information, in the form of MIB Object Identifiers (OIDs), is sent from your storage system's agent to an SNMP management station.

About built-in traps in Data ONTAP MIBs

Built-in traps in Data ONTAP MIBs are identified by the string TRAP-TYPE. For example, the following is a complete trap definition from the Data ONTAP custom MIB:

```
upsLinePowerOff          TRAP-TYPE
ENTERPRISE               netapp
DESCRIPTION
     "UPS: Input line power has failed and UPS is now on battery."

::= 142
```

Traps in the custom MIB are provided in a number of categories, including the following.

Category	Examples of trap messages
Disk Health Monitor	Degraded I/O, disk predictive-failure event
Disks	Disk - failure alert, shutdown, repaired
Fan	Fan - failed, shutdown, warning, repaired
Power supply	Power supply - failed, shutdown, warning, repaired
CPU	CPU busy, OK
NVRAM	Battery discharged, low
Cluster	Node failed, repaired
Volumes	Nearly full, full, repaired

Category	Examples of trap messages
Temperature	Over temperature, shutdown, repaired
Shelf	Fault, repaired
Global	Not recoverable, critical, not critical, OK
Soft quotas	Exceeded, normal
Autosupport	Send error, configuration error, successful send

Note

These categories are examples of the MIB trap contents; it is not an exhaustive list. The most complete listings are provided in the MIBs themselves.

About MIB trap priority

By convention, the right-most digit of a trap ID number indicates its priority (degree of severity), using the same enumeration as syslog entries. For example, trap ID 142 `upsLinePowerOff` is priority 2, alert.

Trap priorities are listed in the following table.

Trap ID last digit	Priority
1	emergency
2	alert
3	critical
4	error
5	warning
6	notification
7	information
8	debug

For more information, see the na_syslog.conf(5) man page.

Where to get further information

See the following RFCs for more information:

- RFC 1157—Defines and describes SNMP.
- RFC 1213—Defines and describes the SNMP MIB-II specification.
- RFC 1155—Defines and describes the structure and identification of management information for TCP/IP-based internets.
- RFC 1215—Defines the convention for defining traps for use with SNMP.
- RFC 1212—Gives concise MIB definitions.